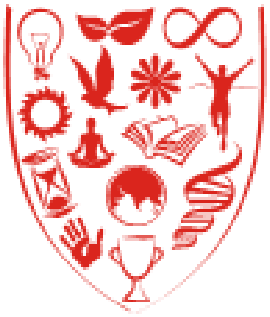
DISTRIBUTED DENIAL OF SERVICE (DDOS) MITIGATION BY BLOCKCHAIN AND SOFTWARE DEFINED NETWORK(SDN)

Research Protocol

Submitted by

Laxmi Poonia

19PHEN033



Under the Guidance of

Dr. Seema Tinker

Professor

JECRC University, Jaipur

2020-21

JECRC UNIVERSITY, JAIPUR

Synopsis

1 Introduction

In the digital age, everything is connected to the internet. While the internet makes the lives easy for billions of users. It has also opened new doorways for mischievous elements for cyber crimes. With a rapidly growing landscape, cyber threats are becoming more dominant. Among these threats, Distributed Denial of Service (DDoS) attacks are very critical and have become a major security threat. This is particularly the case with the increasing number of interconnected devices and systems, such as the Internet of Things (IoT) and Software-Defined Networking (SDN). In simple terms, it is an attack that tends to flood any given network, service, or infrastructure with excessive traffic, thus overloading it and making access for genuine users almost unattainable. This is because, through the rise in frequency, scale, and complexity, DDoS attacks would seriously threaten the stability and security of contemporary networked systems to the point of causing significant financial losses, reputational damage, and service interruptions, among others (Zargar et al., 2013).

Classic methodologies of detecting and mitigating DDoS attacks use centralized architectures in view of predefined rule-based systems, and such rules turn out to be less efficient when attacked with more complex and dynamic attack strategies. In addition, though SDN provides advanced network programmability and flexibility, it is centralized in nature, hence introducing a single point of failure, making it highly prone to DDoS attacks (Kreutz et al., 2015). In IoT environments, the presence of numerous heterogeneous devices having different levels of security complicates the detection and mitigation processes because these devices often do not have enough computational power to implement full-fledged security measures(Kumar et al., 2022).

Blockchain technology proves to be beneficial due to its decentralized, transparent, and tamper-proof platform that can be leveraged to implement cybersecurity (Zheng et al., 2017). With the help of a distributed ledger, it can ensure integrity and availability, which is the reason it holds promise for constructing resilient security frameworks. Being integrated into an SDN framework, blockchain technology allows for the solving of the single point of failure problem by the mechanism of control decentralization and provides a safety protocol for interactions among

devices located on the network. However, this is a place that will require careful handling, as the computational demands of blockchain operations themselves and concerns about scalability in wide-area networks cannot be ignored (Gatteschi et al., 2018).

Conversely, it has now been established that machine learning is a robust method of detecting anomalies and, by the same token, making predictive analytics in cybersecurity. ML models can detect patterns showing malicious activity, for example, DDoS attacks, trained on historical data. On one side, supervised learning techniques, such as support vector machines and decision trees, have been found to effectively recognize known attack patterns, while unsupervised techniques, like clustering and auto-encoders, are efficient in detecting novel or evolving threats (Sommer & Paxson, 2010). However, ML models can suffer from high false positive rates, and in dynamic environments such as SDN and IoT, they may require substantial computational resources for real-time analysis (Nguyen & Armitage, 2008).

2 Problem Statement

The modern network infrastructures have been radically changed by the wide adoption of the technologies behind Software-Defined Networking and Internet of Things. These bring in enhanced flexibility, scalability, and centralized control, but these same technological advancements open the doors to a series of important security challenges. While SDN's centralized control plane enhances the capability for better network management, at the same time, it creates a single point of failure, which is an attractive proposition for attackers to target the network. In this respect, its diversified nature and resource-constrained devices in the context of IoT present vulnerabilities that are hard to guard against in large-scale DDoS attack attempts. Traditional techniques for detecting and mitigating DDoS attacks involve centralized architectures with predefined rule-based systems. These traditional approaches become more and more inadequate for confronting the complications and dynamics of modern DDoS attacks, which grow in sophistication, scale, and unpredictability. Furthermore, integrating blockchain technology brings along other challenges, such as computational overhead and concerns for scalability, to be managed. There is hence an increasing demand for developing innovative, decentralized, and scalable solutions using emerging technologies such as Blockchain and Machine Learning in the detection and mitigation of DDoS attacks within SDN and IoT environments.

3 Research Objectives

The following research objectives are designed to address the identified challenges in detecting and mitigating DDoS attacks:

- To study and analyze DDoS mitigation techniques, including the use of blockchain technologies and Software Defined Networks (SDN).

- To investigate distinct types of DDoS attacks, including their classifications, impacts, and associated prevention and mitigation strategies.

- To evaluate and investigate the performance of Software Defined Networks (SDN) in mitigating DDoS attacks.

- To assess and investigate the effectiveness of blockchain technologies in mitigating DDoS attacks.

4 Literature Survey

4.1 DDoS Attack

An attempt to prevent a network, service, or website from functioning normally by saturating it with internet traffic is known as a distributed denial of service (DDoS) attack. These attacks are carried out employing numerous compromised PCs as attack traffic sources. The devices involved in delivering the malicious traffic are often distributed globally, creating challenges in defending against these attacks. The basic schematic for a DDoS attack is shown in Fig. 1. It can be seen that it has four different components, namely an Attacker, numerous slaves, agents, and a target machine. The DDoS attack is carried out in three stages: gathering of the army, preparation of the army, and launch.

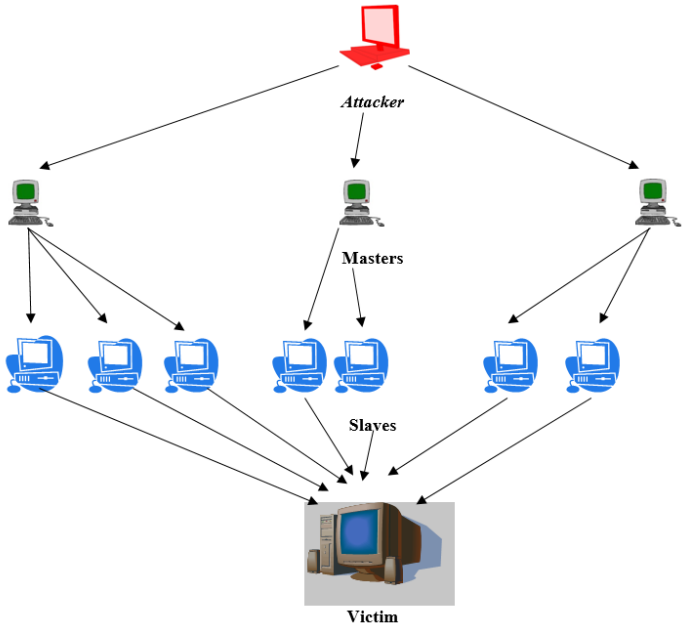


Figure 1: Basic working of DDoS attack

- **Gathering:** Initially, the attacker identifies and compromises a single machine on the network. This machine is known as the master or handler. The attacker spends a lot of time on the compromised machine to exploit a significant number of machines to build an attacking army using the security loopholes, and proceeds to install the malicious code on the machine to be attacked.

- **Preparation:** After gathering a sufficient number of devices for the attack, known as a botnet. The attacker sends all the required information, like codes, commands, and multiple requests, to the master armies. The slave armies are asked to prepare for an attack by the master armies.
- **Launch:** The attacker gives instructions to its army to initialize and execute the attacks. They attack the victim's machine in a distributed way by sending a large number of requests to the victim system, which turns into a flood of major resources.

4.2 Characteristics and Impact of DDoS Attack

DDoS attacks have also progressed significantly from their early versions and have become more sophisticated, massive, and destructive. These attacks traditionally aim at saturating the target system with excess traffic so that the system will be incapacitated in terms of its response toward legitimate users. In the initial days of DDoS, the attacks were relatively simple and commonly employed a single attack vector, such as ICMP or SYN flooding. Still, today's DDoS attacks implement multiple vectors, which can be a blend of volumetric attacks, protocol-based attacks, and application layer attacks (Zargar et al., 2013).

The consequences of DDoS attacks on network infrastructures are significant, most of the time creating considerably large service disruptions, financial losses, and damage to the reputation. Research shows that the average cost related to a DDoS attack can run into hundreds of thousands of dollars for every hour of downtime. Additionally, growing dependency on cloud services and reaching-out penetration of IoT devices have also enlarged the attack surface, making it easier for attackers to deploy large-scale DDoS attacks. The emergence of botnets like Mirai was seen using IoT devices to carry out massive DDoS attacks, which has shown the growing threat these attacks possess (Zheng et al., 2017). As tactics for DDoS continue to evolve and start to attack critical infrastructure, there is a pressing need for the development of more advanced strategies for detection and mitigation.

4.3 SDN and IoT Vulnerabilities

Software-defined networking (SDN) and the Internet of Things (IoT) are two pivotal advancements in contemporary networking. SDN makes it possible to separate a data plane from

a control plane, enabling centralized network management for flexibility. However, this centralization leads to a single point of failure and exposes the SDN controllers strongly to DDoS attacks (Kumar et al., 2022). An attack on the controller can be successful in taking down the whole network; thus, security enforcement is an important issue for the SDN architecture.

The IoT, with its massive scale of interconnected devices, comes with a unique set of challenges. Most devices used in IoT implementation are resource-constrained and hence are, by large, devoid of proper security features. This leads to compromise quite easily, and subsequent utilization in DDoS attacks has been on the increase. In addition, detection and mitigation of attacks within the IoT are further complicated by the heterogeneous nature of IoT devices and the lack of standardized security protocols (Wani et al., 2021). A good example is the Mirai botnet, which used insecure IoT devices to carry out one of the largest DDoS attacks in history (Shah et al., 2022). The inherent vulnerabilities in SDN and IoT both, therefore, necessitate the development of an integrated security framework to bring out a solution to these unique challenges that they currently face.

4.4 Blockchain in Cybersecurity

The decentralized, transparent, and tamper-resistant properties of a blockchain are what attract interest in its application to cybersecurity. While it was initially developed as an underlying framework for cryptocurrencies like Bitcoin, blockchain technology is now under research for many different applications, including secure communications, identity management, and, importantly, DDoS mitigation (Mousavi & St-Hilaire, 2015).

The decentralized design of the blockchain completely removes the single point of failure, making it a very good solution for attaining secure network infrastructures in cybersecurity. Distributed ledgers of network transactions can be set up using the blockchain; these ledgers can further be analyzed for abnormal activities that could possibly signal DDoS attacks. Blockchain records are immutable, meaning that once data has been recorded, it is impossible to change it, thus providing a tamper-proof audit trail—something beyond value for forensic analysis after an attack (Nguyen & Armitage, 2008). Other valuable, additional functions include responses to detected threats, such as automatic isolation of compromised devices or rerouting traffic, in the case of smart contracts, which are self-executing agreements with terms directly encoded.

However, the integration of blockchain with cybersecurity frameworks gives rise to several challenges, mostly related to the computational demand of blockchain operations. Consensus mechanisms, such as proof-of-work, can bring up issues with latency and scalability (Kshetri, 2017). This forms a challenge to be tackled to make use of blockchain technology for cybersecurity purposes, in order to detect and prevent DDoS attacks.

4.5 Machine Learning for Anomaly Detection

Machine learning, as a vital technology of network security, has found active implementation in anomaly detection and further mitigation of distributed denial of service attacks. ML models can process huge datasets of network traffic information to identify patterns of activity that deviate from regular behavior, signaling a potentially ongoing attack. In this regard, a variety of ML techniques—ranging from supervised to unsupervised and reinforcement learning—have been used with various levels of success (Halladay et al., 2022).

Specifically, for DDoS detection, supervised learning algorithms such as Support Vector Machines or Decision Trees are used. For these kinds of models, labeled datasets are required, through which the system is trained to discriminate between normal traffic and an attack. But this can be a downside for many applications because labeled data is sometimes not available or comprehensive enough. These are unsupervised techniques, such as clustering methods or anomaly detection models, that are used for identifying novel and emerging threats. Such techniques find utility in dynamic environments, such as SDN and IoT, where patterns of attacks might change very fast (Kokoris-Kogias et al., 2016).

Reinforcement learning, which involves training an agent to make decisions through trial and error, has also been explored for DDoS mitigation. This approach can be used to dynamically adjust security measures in response to detected threats, improving the network's defense mechanisms over time. Despite the potential of ML in anomaly detection, challenges remain, particularly in minimizing false positive rates and ensuring the capability for real-time processing.

4.6 Hybrid Approaches: Combining Blockchain and Machine Learning

The blending of blockchain with machine learning is a new strategy to advance cybersecurity. Mainly, it is made based on DDoS detection and mitigation. Blockchain ensures that the data stored

and shared on a network are secure and decentralized, while machine learning furnishes deep tools for the detailed analysis of that information in a bid to detect anomalies and predict potential threats (He et al., 2017).

5 Methodology

The proposed study will aim to develop novel frameworks to detect and mitigate DDoS attacks. An example of the proposed methodology is shown in Figure 2 below.

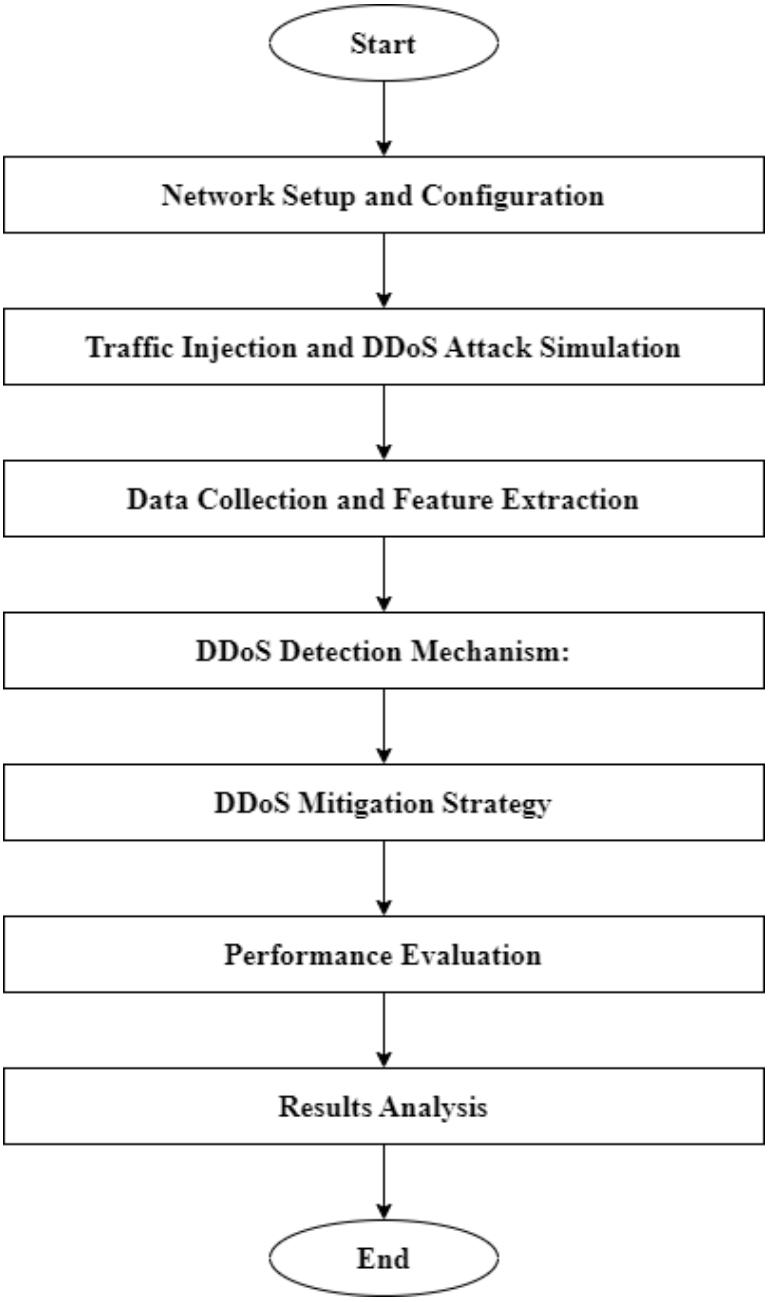


Figure 2 Proposed Methodology

1. **Network Setup and Configuration**

   - Define the Network Topology: Establish a network topology, i.e., an SDN network, using simulation software, such as Mininet, or something functionally equivalent. This involves the configuration of switches, hosts, and the SDN controller.

- Deploy the network, that is, implement an SDN controller (e.g., Ryu, ONOS) to manage the flows of the network and guarantee traffic monitoring.

2. **Traffic Injection and DDoS Attack Simulation**

   - Generate Normal Traffic: Inject normal network traffic into the environment to simulate regular network operations.

   - Simulate DDoS Attack: Introduce DDoS attacks into the network to simulate a real-world attack scenario.

3. **Data Collection and Feature Extraction**

   - Monitor Traffic at Edge Switches: Collect traffic data from edge switches in the network.

   - Extract Features: Extract relevant features from the collected data, such as packet count, flow rate, and source IP address distribution.

4. **DDoS Detection Mechanism**

   - **SDN-Based Mitigation**: An SDN controller will be used to dynamically reconfigure the network in response to detected DDoS attacks, isolating and mitigating malicious traffic while minimizing disruption to legitimate users.

   - **Blockchain-Based Detection**: A decentralized system that records network activities on a blockchain, providing a tamper-proof log of all network events. Smart contracts will be used to automate the detection and reporting of suspicious activities.

   - **Machine Learning Models**: Development of machine learning algorithms that analyze the blockchain logs and network traffic data to detect anomalies indicative of DDoS attacks. These models will be trained using both historical data and real-time traffic.

5. **DDoS Mitigation Strategy**

- Deploy Mitigation Techniques: Upon detection, the SDN controller enforces mitigation techniques such as updating flow tables to block malicious traffic, rate limiting, or rerouting traffic.
- Real-time Monitoring: Continuously monitor the traffic and adjust mitigation strategies as needed.

6. Performance Evaluation

- Evaluate Detection Accuracy: Measure the accuracy of the detection module by comparing it to the baseline detection accuracy.
- Measure Controller Load: Evaluate the CPU utilization of the SDN controller under different scenarios (e.g., with and without attack, different mitigation strategies).

7. Result Analysis

- Analyze CPU Utilization: Compare the CPU utilization of the proposed system with a centralized detection system.
- Effectiveness of Mitigation: Assess the effectiveness of the mitigation strategies in reducing the impact of the DDoS attack.

6 Limitations

Various limitations restrict our outcomes. A few of them are identified so far and listed below:

1. First and foremost, the significant computational resources required for real-time processing and decision-making posed a major challenge. Each of these technologies, i.e., SDN for dynamic network management, blockchain for secure and decentralized logging, and machine learning for anomaly detection, demands substantial computational power when operated independently, and the integration of these systems would exponentially increase this requirement.

2. The complexity of ensuring seamless communication and interoperability between the different systems further complicated the integration process. Blockchain's inherent latency and high operational costs, particularly when executing smart contracts in a real-time environment, conflicted with the need for rapid response times essential for mitigating DDoS attacks. Similarly, machine learning models, while effective in detecting complex patterns, require extensive training datasets and optimized algorithms, which were difficult to harmonize with the SDN controller's need for immediate and efficient traffic management.

Given these resource limitations, we choose to develop and evaluate these technologies as independent components, recognizing that while their integration holds promise, it remains a challenge for future work when sufficient resources and optimizations can be allocated to overcome these barriers.

7 Expected Outcomes

The research is expected to produce the following outcomes:

- **Comprehensive understanding of DDoS mitigation techniques**: A detailed analysis of current DDoS mitigation strategies, focusing on the role of blockchain technologies and Software Defined Networks (SDN).
- **Enhanced knowledge of DDoS attacks**: A thorough classification and evaluation of various DDoS attacks, including their impacts and the effectiveness of existing prevention and mitigation methods.
- **Improved performance of Software Defined Networks (SDN) for DDoS mitigation**: Identification of areas for optimizing SDN capabilities, leading to better performance and resilience against DDoS attacks.
- **Enhanced effectiveness of blockchain technologies for DDoS mitigation**: Development of optimized approaches to utilize blockchain technology more efficiently for mitigating DDoS attacks, contributing to overall network security.

References

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*, *10*(2). https://doi.org/10.3390/fi10020020

Halladay, J., Cullen, D., Briner, N., Warren, J., Fye, K., Basnet, R., Bergen, J., & Doleck, T. (2022). Detection and Characterization of DDoS Attacks Using Time-Based Features. *IEEE Access*, *10*, 49794–49807. https://doi.org/10.1109/ACCESS.2022.3173319

He, Z., Zhang, T., & Lee, R. B. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 114–120. https://doi.org/10.1109/CSCloud.2017.58

Kokoris-Kogias, E., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016). Enhancing bitcoin security and performance with strong consistency via collective signing. *Proceedings of the 25th USENIX Conference on Security Symposium*, 279–296.

Kreutz, D., Ramos, F. M. V, Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, *103*(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/https://doi.org/10.1016/j.telpol.2017.09.003

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55–68. https://doi.org/https://doi.org/10.1016/j.jpdc.2022.01.030

Mousavi, S. M., & St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. *2015 International Conference on Computing, Networking and Communications (ICNC)*, 77–81. https://doi.org/10.1109/ICCNC.2015.7069319

Nguyen, T. T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, *10*(4), 56–76. https://doi.org/10.1109/SURV.2008.080406

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, *22*(3). https://doi.org/10.3390/s22031094

Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry*, *13*(2). https://doi.org/10.3390/sym13020227

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85